УДК 004.922 Вестник УрФО № 1(51) / 2024, с. 45–52

Грибачёв А.С., Кальщиков В.В., Ручай А.Н. DOI: 10.14529/secur240106

МЕТОДЫ, АЛГОРИТМЫ И БАЗЫ ДАННЫХ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ

В современных реалиях, передача, обработка и хранение информации производится преимущественно в электронном виде. Процесс обработки и анализа электронных данных происходит куда быстрее и удобнее и, что не мало важно, намного дешевле: достигается это благодаря хранению информации в специализированных базах данных. Цифровизация – это современный инструмент, позволяющий человеку получать интересующую его информацию за короткий промежуток времени. Использование продуктов цифровизации позволяет более рационально использовать время, однако, информация о человеке более уязвима. Сегодня мы можем наблюдать как информация подвергается различным мошенническим атакам: телефонные мошенники, целью которых является банковские сведения человека, шпионское программное обеспечение внедряется для использования компьютерных мощностей пользователя для преступных целей, кража личной информации и переписки в социальных сетях для последующей публикации в открытом доступе и, как следствие, серьезный урон репутации человека или компании. Часто бывает так, что данным угрожают не злоумышленники, а недостаточно квалифицированные пользователи, либо ошибки в программном обеспечении, что в обоих случаях, приводит к потери информации. Огромное количество угроз в цифровой сфере обосновывает необходимость обеспечивать не только доступность цифровых сервисов, но и их безопасность. Обеспечение защиты информации на объектах критической информационной инфраструктуры для страны является одной из главных задач. Поэтому превентивная защита, своевременная реакция на данные виды атак, а также принятие мер по противодействию киберугрозам является приоритетной задачей. Цель данной работы состоит в изучении типов компьютерных угроз, существующих типов баз данных, методов обнаружения кибератак и способов противодействия им.

Ключевые слова: *кибербезопасность, критическая информационная инфраструктура, обнаружение атак, информационная безопасность, машинное обучение, базы данных.*

Gribachev A.S., Kalshikov V.V., Ruchay A.N.

METHODS, ALGORITHMS AND DATABASES FOR DETECTING COMPUTER INCIDENTS

In modern realities, the transfer, processing and storage of information is carried out digitally. Processing and analyzing digital data are much faster and more convenient and much

cheaper: this is achieved by storing information in specialized databases. Digitalization is a modern tool that allows a person to obtain interest information in a short period of time. The use of digitalization products allows for more efficient use of time, however, information about a person is more assailable. Today information is subjected to various scam attacks: phone scammers whose goal is a person's banking information, spyware is introduced to use the user's computer power for criminal purposes, theft of personal information and correspondence in social networks for publication in the public domain, and, as a result, serious damage to the reputation of a person or company. Often, data is threatened not by attackers, but by insufficiently qualified users, or by software errors, which in both cases leads to loss of information. The huge number of threats in the digital sphere justifies the need to ensure not only the availability of digital services, but also their security. Ensuring the protection of information at objects of critical information infrastructure for the country is one of the main tasks. Therefore, preventive protection, timely response to these types of attacks, as well as taking measures to counter cyber threats are a priority. The purpose of this work is to study the types of computer threats, the types of databases, methods of cyberattacks detection and ways to counter it.

Keywords: *cybersecurity, critical information infrastructure, attack detection, information security, machine learning, databases.*

Введение

Сегодня превентивная защита и принятие мер по обнаружению и предотвращению киберугроз на информационные системы и компьютерное оборудование предприятий, на объекты критической информационной инфраструктуры одна из важнейших задач по обеспечению информационной безопасности страны. [1-2] Активное внедрение технологии интернета вещей в жизнь современного человека, цифровизации различных бизнес-процессов учреждений и предприятий, все это упрощает и облегчает существование и функционирование в различных сферах деятельности общества: медицина, сельское хозяйство, экономика и многие другие. Однако, это также является благоприятной средой для киберпреступности, что подтверждается каждодневным ростом кибератак на объекты критической информационной инфраструктуры. Кибератака представляет собой определенное действие, которое связанно с проникновением в компьютерную систему, минуя систему защиты. Обнаружение такого незаконного неавторизованного доступа в систему называют выявлением кибератаки. [3] Статья представлена в 4 разделах: 1, 2 и 3 разделы посвящены кибератакам и методам их обнаружения, в 4 разделе приводится обзор имеющихся структур баз данных, использующихся в построении SIEM-систем, а также примеры наборов данных современных атак.

Виды и типы кибератак на критическую информационную инфраструктуру

Действия киберпреступников направлены на получение несанкционированного доступа к информационным системам и каналам связи инфраструктуры для перехвата управлением, либо получения данных, имеющих определенную ценность. [4] Такие действия подразделяются на два вида: целевые и распределенные кибератаки. Одни нацелены на определенную компанию или отрасль, такой вид атаки подразумевает получение доступа к ресурсам инфраструктуры и минимизация риска обнаружения киберпреступника в системе, то есть злоумышленник может находиться в сети долгое время, до момента его обнаружения. Для реализации такого типа атак необходимы автоматизированные инструменты и высокоспециализированные хакеры. Другие направлены на огромное количество информационных систем компаний, для таких атак применяются специальные роботизированные сети.

Существуют различные типы атак на критическую информационную инфраструктуру:

1. Боты. Происходит имитация поведения человека, однако робот выполняет задачи быстрее самого пользователя. Доступность ботов и их возможность совершать огромное количество атак одновременно существенно упрощает работу злоумышленникам. Киберпреступники применяют комбинированный подход при обходе механизмов защиты информационных систем от ботнетов, то есть используют комбинацию автоматизированных скриптов и действий реального человека. Такие гибридные кибератаки гораздо сложнее обнаружить. Зачастую ботов исполь-

зуют для подготовки к атаке, для сбора информации и создания информационной базы. Проводятся направленные кибератаки с максимальной имитацией действий человека, таким способом избегают блокировок системой защиты. Современные боты могут очень точно имитировать действия реального человека благодаря применению технологии машинного зрения.

2. Атака «грубой силой» – представляет собой метод получения доступа в информационную систему путем взлома учетных записей. Получив данные адресов электронной почты или имена пользователей информационных систем, злоумышленник методом перебора паролей пытается получить доступ к таким системам. Обычно используются специализированное программное обеспечение, позволяющее создавать списки учетных данных для аутентификации. Данный вид атаки требует значительных временных трат, так как перебор всех возможных комбинаций имен пользователей и паролей до тех пор, пока не будет найдена корректная требует времени. Применение парольной политики и ограничивая количество запросов на авторизацию для одного аккаунта и с одного IP-адреса можно существенно снизить успешность атаки «грубой силы» на информационные ресурсы.

3. Отказ в обслуживании - эти атаки нагружают систему большим количеством запросов, в результате происходит снижение пропускной способности, а система недоступной. Данный тип кибератак относится к типу сетевых атак. Возможны два варианта реализации такого рода атак: отправка огромного объема данных с такой скоростью, что их обработка станет невозможной, либо могут передаваться пакеты данных, в которых содержатся ошибки, при обработке таких данных системы тратят много времени, начинают работать медленно и выходят из строя. Основными способами защиты от «DDoS-атак» является уменьшение зон, доступных для атаки, анализ сетевого трафика, увеличение пропускной способности и производительности серверов, достаточной для нейтрализации и поглощения кибератак.

4. Фишинг – использование почтовых рассылок, замаскированных под обычные сообщения компании, либо создание поддельных страниц регистрации с целью получения идентификационных данных. Для атак на критическую информационную инфраструктуру может быть использован направленный фишинг, то есть нацеленная рассылка на определенный объект или организацию. В качестве защиты от фишинга необходимо использовать надежную систему защиты, применять двухфакторную аутентификацию в системах, применять парольную политику, при передаче данных внимательно изучать сетевые-ресурсы и почтовых отправителей.

5. Атака через посредника. При таком типе атаки в момент передачи сообщений происходит утечка данных третьей стороне. [5-10] Киберпреступники, перехватывая трафик, могут перенаправлять его, либо пропускать, анализирую информацию в момент ее поступления. Злоумышленник выступает в роли посредника между отправителем и адресатом. Такой вид атак очень распространен, например в общедоступных сетях. Также в целях шпионажа или кражи данных могут быть установлены мошеннические точки доступа даже в частных сетях. IP, ARP, DNS, HTTPS, SSL спуфинги, перехват сеансов, внедрение пакетов, SSL-стриппинг применяются для подмены данных и передачи их злоумышленнику. Защита от такого типа угроз представляет собой полный отказ от использования общедоступных сетей при работе с конфиденциальной информацией, использование стойкого шифрования при передаче данных между клиентом и сервером, а также аудит локально-вычислительных сетей на наличие несанкционированного оборудования.

Методы обнаружения кибератак

Современные системы обнаружения кибератак основываются на сборе данных о трафике сетевых соединений и журналируемых событиях серверов и ключевых компьютеров. Такие системы проводят наблюдение и анализируют события, которые происходят в информационной инфраструктуре, а также позволяют отслеживать различные сетевые атаки, такие как проникновение в сеть, отказ в обслуживании и сканирование портов. Анализ различных системных характеристик, либо отслеживание входящего/исходящего трафика позволяет обнаружить вредоносные действия. [11-12]

Методы обнаружения компьютерных угроз можно разделить на следующие блоки:

• Сигнатурный анализ базируется на рассмотрении содержимого исследуемого объекта сигнатур уже известных угроз. Для возможности обнаружения угрозы исследуются ее характерные признаки. Сравнение проис-

ходит по контрольным суммам. Такой подход значительно снижает размер записей в базах и позволяет сохранить корректность обнаружения угроз.

• Метод эмуляции исполнения. Основное применение заключается в детектировании полиморфных и шифрованных вирусов. Применяется специальная программная модель процессора и эмулятор (среда исполнения программ). Эмулятор работает с буфером эмуляции, при этом инструкции не передаются на центральный процессор для реального исполнения.

• Эвристический анализ основывается на наборе эвристик о характерных признаках вредоносного и безопасного исполняемого кода. Каждому признаку такого кода назначается определенный вес. Исходя из суммарного веса, эвристический анализатор производит расчет вероятности, что в исследуемом объекте содержится неизвестный код. Если такая вероятность превышает пороговое значение, то будет выдано заключение - анализируемый объект является вредоносным.

• Метод поведенческого анализа позволяют анализировать последовательность действий всех процессов в системе. При обнаружении признаков поведения вредоносной программы действия приложения блокируются.

• Метод машинного обучения. Данный метод используется для обнаружения угроз, которые отсутствуют в вирусных базах. Преимущество метода – распознавание угроз на основе их характеристик. Основывается на классификации кибератак согласно определенным признакам. Метод машинного обучения позволяет экономить ресурсы операционной системы, так как не требует исполнения кода для выявления угроз. [13-14]

Исследование систем обнаружения и предотвращения вторжений

Системы обнаружения вторжений представляют собой программные, либо программно-аппаратные средства, позволяющие выявлять факт неавторизованного, несанкционированного доступа к устройству.

Архитектура систем обнаружения вторжений включает:

• сенсорную подсистему, которая предназначена для сбора входящего трафика, регистрации событий, связанных с безопасностью защищаемой системы

• подсистему анализа, которая предназначена для определения кибератак и подозрительных действий на основе поступающих данных от сенсорной подсистемы

• хранилище, в котором накапливаются и систематизируются первичные события и результаты анализа

• консоль управления, которая позволяет сконфигурировать систему обнаружения вторжений, наблюдать за состоянием защищаемой системы и просматривать выявленные подсистемой анализа инциденты.

Возможны следующие исполнения системы обнаружения вторжений: сетевая, основанная на протоколах связи, основанная на прикладных протоколах, узловая и гибридная. [15]

Для реализации анализа могут применяться различные технологии. Изначально для обеспечения защиты применялись простые политики. Например, при превышении определенного количества данных передача таких данных либо полностью останавливалась, либо нуждалась в дальнейшем подтверждении. Анализ сигнатур позволяет сравнивать данные, которые собраны сенсорами с имеющимися базами киберугроз. Анализ аномалий позволяет вычислять необычные действия без заранее созданных баз данных. Например, поведенческий анализ, который может определить отклонение от статистических метрик и количества действий, найти аномалии в самом трафике или протоколах связи.

Существуют различные способы обнаружения попыток вторжения в информационную инфраструктуру: сетевой трафик, активность портов, в данных, которые передаются по отслеживаемым протоколам, а также на конечных узлах. В зависимости от способа установки и технологии анализа системы обнаружения и предотвращения вторжений способны детектировать действия вредоносного программного обеспечения, использование ботнетов для атаки, попытки несанкционированного доступа к защищаемым данным, а также нарушение правил и политики безопасности.

Базы данных и наборы данных

Для предотвращения потери информации под действием кибератак широко используются SIEM-системы. Для разработки SIEM-системы используются различные типы существующих баз данных. Базами данных называют упорядоченные наборы структурированных данных. В компьютерных системах такие данные хранятся в электронном виде.

Для управления базами данных применяется инструмент - система управления базами данных (СУБД). В современных типах баз данных принято хранить данные в виде столбцов и строк, которые образуют таблицы. Применяя такой метод хранения данных, намного проще совершать над ними различные операции: добавлять, изменять, удалять, обновлять, отслеживать и систематизировать. При обращении к данным (для осуществления записи или выполнения запросов к таких данных) в большинстве современных баз данных используется язык SQL (структурированные запросы).

При выборе базы данных под разработку конкретной SIEM-системы очень важно учитывать с какими данными придется работать и как они будут использоваться, какая будет структура у таких данных. Таким образом, важно понимать какой тип баз данных будет использоваться.

Рассмотрим простейшие типы баз данных:

1. Простые структуры данных. Простым способом хранения данных являются текстовые файлы. Управлять разделением полей можно используя специальный символ: запятую, точку с запятой, двоеточие или пробел.

2. Иерархические базы данных. Основным отличием от простых структур является появление связей между объектами. Каждая запись, в такой структуре, имеет одного родителя и классифицируется в соответствии с тем, как она относится к родительской цепочке записей.

3. Сетевые базы данных. Записи таких баз данных могут иметь более одного родителя, что позволяет моделировать более сложные взаимосвязи.

4. Реляционные базы данных. Организация данных в реляционных базах представлена в виде таблиц, состоящих из столбцов и строк. Столбцы таблиц реляционных баз данных имеют имена и типы, а строки в свою очередь представлены отдельными записями, которые содержащат определенное значение для каждого из столбцов.

5. Базы данных NoSQL. Предназначены для работы в веб-приложениях реального времени и больших данных. Высокая доступность и масштабируемость являются основными преимуществами баз данных NoSQL.

6. Комбинированные базы данных. Разновидность баз совмещает в себе SQL- и NoSQL-подходы к организации хранения и обработки данных. Этот класс баз включает в себя NewSQL и многомодельные решения.

7. Объектно-ориентированные базы данных – базы данных, в которых информация представлена в виде объектов, как в объектно-ориентированных языках программирования.

8. Облачная база данных — это совокупность структурированных или неструктурированных данных, размещенных на частной, общедоступной или гибридной платформе облачных вычислений.

Набор данных или датасет — это коллекция данных, которая касается определенной темы или отрасли. Наборы данных включают различные типы информации: текст, изображения, видео и аудио, и могут храниться в различных форматах, таких, как CSV, JSON или SQL. [16]

Например, набор данных CICIDS2017 содержит безопасные и самые современные распространенные атаки. Включают результаты анализа сетевого трафика с использованием CICFlowMeter с маркировкой потоков. (файлы CSV). [17] А в наборе данных CSE-CIC-IDS2018 авторы используют понятие профилей для систематического создания наборов данных, которые будут содержать подробные описания вторжений и абстрактные модели распространения для приложений, протоколов или сетевых объектов более низкого уровня. Эти профили смогут использоваться агентами или операторами для генерации событий в сети. [18] Набор данных UNSW-NB 15 содержит девять типов атак, а именно: фаззеры, анализ, бэкдоры, DoS, эксплойты, общие, разведывательные, шеллкоды и черви. [19]

Заключение

В данной работе рассмотрены различные типы компьютерных угроз, а также методы их обнаружения, а также рассмотрены структуры баз данных, которые могут применяться при построении SIEM-систем. Рост требований скорости работы и производительности систем привел к увеличению количества типов баз данных. Перед началом создания SIEM-системы необходимо выбрать тип используемой базы данных, а для этого необходимо учитывать не только удобство хранения, но и скорость получения и использования данных. Используя связи нескольких баз данных, можно сохранить удобство хранения данных и их классификацию, а также высокую скорость получения больших объемов информации за счет предварительной индекса-

ции. Анализ существующих наборов данных кибератак позволяет обобщить их основные характеристики и использовать в дальнейших исследованиях. Важными составляющими методов обнаружения аномалий поведения информационных систем являются анализ последовательности действий всех процессов и классификация угроз по определенным характеристикам и признаками. Для повышения эффективности важно достижение оптимальных значений достоверности, точности и снижения времени принятия решений, что возможно лишь с применением глубокого машинного обучения. Одним из возможных путей решения проблемы обнаружения угроз - применение систематизации данных угроз, что позволит понять технологию обнаружения этих атак и разработать метод их обнаружения.

Литература

1. Доктрина информационной безопасности Российской Федерации. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646.

2. Хлопов О.А. Проблемы кибербезопасности и защиты критической информационной инфраструктуры. Political Sciences. The scientific heritage № 45, 2020.

3. Серёдкин С.П. Особенности кибератак на объекты критической информационной инфраструктуры в современных условиях. Информационные технологии и математическое моделирование в управлении сложными системами. Электрон. науч. журн. №4(16), 2022, с. 56-66.

4. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. /В. Ф. Шаньгин//, Москва: ДМК Пресс, 2012. – 592 с.

5. Путято М.М., Евглевский В.Ю., Макарян А.С., Володин И.В. Исследование механизмов социальной инженерии и анализ методов противодействия. Научные труды КубГТУ, 2021, № 2. С. 57-68.

6. Н.С. Афанасьева, Д.А. Елизаров, Т.А. Мызникова. Классификация фишинговых атак и меры противодействия им. Инженерный вестник Дона, №5, 2022.

7. Баженов А.С. Обзор DDoS атак на IoT устройства. Наука настоящего и будущего, 2019, С. 122-125.

8. Савченко Е.В., Ниссенбаум О.В. Ботнет-атаки на устройства интернета вещей. Математическое и информационное моделирование. Сборник научных трудов, электронный ресурс. Тюмень, 2018, С. 347-356.

9. Ручай А.Н., Токарев И.В., Грибачёв А.С. Методы машинного обучения и искусственного интеллектав сфере информационной безопасности: анализ современного состояния и перспективы развития. Вестник УрФО No 4(46), 2022, С. 76–87.

10. Грибачёв А.С., Кальщиков В.В. Исследование методов и алгоритмов обнаружения компьютерных инцидентов. Сборник трудов XXII Всероссийской научно-практической конференции студентов, аспирантов и молодых учёных. Безопасность информационного пространства. Челябинск, 2024, С. 290-293.

11. Крейсат А., Гондал И., Вамплью П. и др. Обзор систем обнаружения вторжений: методы, наборы данных и проблемы. Кибербезопасность 2, 20, 2019.

12. Rafal Kozik, Michal Choraś, Rafal Renk, Witold Holubowicz. A Proposal of Algorithm for Web Applications Cyber Attack Detection. 13th IFIP International Conference on Computer Information Systems and Industrial Management (CISIM), Nov 2014, Ho Chi Minh City, Vietnam. pp.680-687.

13. Г. Ван, Дж. Хао, Дж. Ма и Л. Хуанг. Новый подход к обнаружению вторжений с использованием искусственных нейронных сетей и нечеткой кластеризации, Приложение Expert Syst,, т. 37, № 9, С. 6225-6232, 2010.

14. Методы обнаружения угроз. Электронный ресурс [https://cdn-download.drweb.com/pub/drweb/windows/server/12.0/documentation/html/ru/index.html?intro_detectionmethods.html]

15. Платонов В. Программно-аппаратные средства защиты информации. М.: Академия, 2013.

16. Нестеров С. А. Базы данных: учебник и практикум для вузов / С. А. Нестеров// Москва: Издательство Юрайт, 2024, — 258 с.

17. Набор данных. Электронный ресурс [https://www.unb.ca/cic/datasets/ids-2017.html]

18. Набор данных. Электронный ресурс [https://www.unb.ca/cic/datasets/ids-2018.html]

19. Набор данных. Электронный ресурс [https://research.unsw.edu.au/projects/unsw-nb15-dataset]

References

1. Doktrina informacionnoj bezopasnosti Rossijskoj Federacii. Ukaz Prezidenta Rossijskoj Federacii ot 5 dekabrya 2016 g. № 646.

2. Hlopov O.A. Problemy kiberbezopasnosti i zashchity kriticheskoj informacionnoj infrastruktury. Political Sciences. The scientific heritage № 45, 2020.

3. Seryodkin S.P. Osobennosti kiberatak na ob"ekty kriticheskoj informacionnoj infrastruktury v sovremennyh usloviyah. Informacionnye tekhnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami. Elektron. nauch. zhurn. №4(16), 2022, s. 56-66.

4. Shan'gin V. F. Zashchita informacii v komp'yuternyh sistemah i setyah. /V. F. Shan'gin//, Moskva: DMK Press, 2012. – 592 s.

5. Putyato M.M., Evglevskij V.Yu., Makaryan A.S., Volodin I.V. Issledovanie mekhanizmov social'noj inzhenerii i analiz metodov protivodejstviya. Nauchnye trudy KubGTU, 2021, № 2. S. 57-68.

6. N.S. Afanas'eva, D.A. Elizarov, T.A. Myznikova. Klassifikaciya fishingovyh atak i mery protivodejstviya im. Inzhenernyj vestnik Dona, №5, 2022.

7. Bazhenov A.S. Obzor DDoS atak na IoT ustrojstva. Nauka nastoyashchego i budushchego, 2019, S. 122-125.

8. Savchenko E.V., Nissenbaum O.V. Botnet-ataki na ustrojstva interneta veshchej. Matematicheskoe i informacionnoe modelirovanie. Sbornik nauchnyh trudov, elektronnyj resurs. Tyumen', 2018, S. 347-356.

9. Ruchaj A.N., Tokarev I.V., Gribachyov A.S. Metody mashinnogo obucheniya i iskusstvennogo intellektav sfere informacionnoj bezopasnosti: analiz sovremennogo sostoyaniya i perspektivy razvitiya. Vestnik UrFO No 4(46), 2022, S. 76–87.

10. Gribachyov A.S., Kal'shchikov V.V. Issledovanie metodov i algoritmov obnaruzheniya komp'yuternyh incidentov. Sbornik trudov XXII Vserossijskoj nauchno-prakticheskoj konferencii studentov, aspirantov i molodyh uchyonyh. Bezopasnost' informacionnogo prostranstva. Chelyabinsk, 2024, S. 290-293.

11. Krejsat A., Gondal I., Vampl'yu P. i dr. Obzor sistem obnaruzheniya vtorzhenij: metody, nabory dannyh i problemy. Kiberbezopasnost' 2, 20, 2019.

12. Rafal Kozik, Michal Choraś, Rafal Renk, Witold Holubowicz. A Proposal of Algorithm for Web Applications Cyber Attack Detection. 13th IFIP International Conference on Computer Information Systems and Industrial Management (CISIM), Nov 2014, Ho Chi Minh City, Vietnam. pp.680-687.

13. G. Van, Dzh. Hao, Dzh. Ma i L. Huang. Novyj podhod k obnaruzheniyu vtorzhenij s ispol'zovaniem iskusstvennyh nejronnyh setej i nechetkoj klasterizacii, Prilozhenie Expert Syst,, t. 37, № 9, S. 6225-6232, 2010.

14. Metody obnaruzheniya ugroz. Elektronnyj resurs [https://cdn-download.drweb.com/pub/drweb/windows/server/12.0/documentation/html/ru/index.html?intro_detectionmethods.html]

15. Platonov V. Programmno-apparatnye sredstva zashchity informacii. M.: Akademiya, 2013.

16. Nesterov S. A. Bazy dannyh: uchebnik i praktikum dlya vuzov / S. A. Nesterov// Moskva: Izdatel'stvo Yurajt, 2024, — 258 s.

17. Nabor dannyh. Elektronnyj resurs [https://www.unb.ca/cic/datasets/ids-2017.html]

18. Nabor dannyh. Elektronnyj resurs [https://www.unb.ca/cic/datasets/ids-2018.html]

19. Nabor dannyh. Elektronnyj resurs [https://research.unsw.edu.au/projects/unsw-nb15-dataset]

ГРИБАЧЁВ Антон Сергеевич, аспирант (соискатель) математического факультета, Челябинский государственный университет. 454001, Челябинск, ул. Братьев Кашириных, 129. E-mail: a.gribachev@yandex.ru.

GRIBACHEV Anton Сергеевич, PhD candidate of the Faculty of Mathematics, Chelyabinsk State University. 454001, Chelyabinsk, st. Brothers Kashirinykh, 129. E-mail: a.gribachev@yandex.ru.

КАЛЬЩИКОВ Всеволод Владимирович, аспирант (соискатель) математического факультета, Челябинский государственный университет. 454001, Челябинск, ул. Братьев Кашириных, 129. E-mail: vkalschikov@gmail.com.

KALSHCHIKOV Vsevolod Vladimirovich, PhD candidate of the Faculty of Mathematics, Chelyabinsk State University. 454001, Chelyabinsk, st. Brothers Kashirinykh, 129. E-mail: vkalschikov@gmail.com

РУЧАЙ Алексей Николаевич, кандидат физико-математических наук, доцент, заведующий кафедрой компьютерной безопасности и прикладной алгебры, Челябинский государственный университет. 454001, Челябинск, ул. Братьев Кашириных, 129; доцент кафедры защиты информации, ФГАОУ ВО «Южно-Уральский государственный университет» (национальный исследовательский университет). 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: ran@csu.ru.

RUCHAY Alexey Nikolaevich, PhD in Physics and Mathematics, Associate Professor, Head of the Department of Computer Security and Applied Algebra, Chelyabinsk State University. 454001, Chelyabinsk, st. Brothers Kashirinykh, 129.; Associate Professor, Department of Information Security, South Ural State University (National Research University), Chelyabinsk, 454080, Chelyabinsk, Lenina avenue, 76. E-mail: ran@csu.ru.